

AD-A087 701

ARMY MATERIEL DEVELOPMENT AND READINESS COMMAND ADEL--ETC F/G 17/2  
PSEUDONOISE SPREAD-SPECTRUM SYSTEMS FOR MILITARY COMMUNICATIONS--ETC(U)  
DEC 79 D J TORRIERI  
CM/CCM-79-9

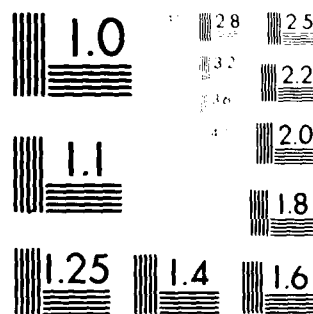
UNCLASSIFIED

NL

1 UP  
40 201-01

U

END  
DATE  
FILMED  
9-80  
DTIC



MICRO COPY RESOLUTION TEST CHART  
NATIONAL BUREAU OF STANDARDS-1963-A

CM/CCM-79-9  
December 1979

7-1  
**LEVEL** ✓

(12)  
D.S.

**Pseudonoise Spread-Spectrum Systems  
for Military Communications**

by Don J. Torrieri

DTIC  
ELECTE  
AUG 11 1980  
S  
C



**U.S. Army Materiel Development  
and Readiness Command  
Countermeasures/  
Counter-countermeasures Office  
2800 Powder Mill Road  
Adelphi, MD 20783**

Approved for public release; distribution unlimited.

ADA 087701

DDC FILE COPY

80 8 8 024

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturers' or trade names does not constitute an official indorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.



Editorial review and camera-ready copy by Technical Reports Branch,  
Harry Diamond Laboratories.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER CM/CCM-79-9	2. GOVT ACCESSION NO. AD-A087701	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Pseudonoise Spread-Spectrum Systems for Military Communications	5. TYPE OF REPORT & PERIOD COVERED Technical Report	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Don J. Torrieri	8. CONTRACT OR GRANT NUMBER(s) DA 1S263749D462	
9. PERFORMING ORGANIZATION NAME AND ADDRESS Countermeasures/Counter-countermeasures Office 2800 Powder Mill Road Adelphi, MD 20783	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Program Ele: 6.37.49.A	
11. CONTROLLING OFFICE NAME AND ADDRESS U.S. Army Materiel Development and Readiness Command Alexandria, VA 22333	12. REPORT DATE December 1979	13. NUMBER OF PAGES 26
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) 12/28	15. SECURITY CLASS. (of this report) Unclassified	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited.		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES ERADCOM Project: T490TB DRCMS Code: 6237494620011		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Pseudonoise      Jamming Spread spectrum      Error probability Direct sequence      Concealment Frequency hopping      Networks Hybrid system      Synchronization		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) The basic characteristics of various pseudonoise spread-spectrum systems are discussed with emphasis on direct-sequence modulation. A necessary condition is derived for the concealment of a pseudonoise waveform from detection. The condition establishes a lower bound for the pseudonoise code length. The bit error probability in the presence of various types of interference is determined. It is shown that if the total bandwidth and the word duration are fixed, the potential improvement in performance due to error-correction coding is partially counterbalanced by the resulting decrease in processing gain. Methods of reducing the mutual interference in a network of pseudonoise systems are examined. Jamming strategies, acquisition techniques, and hybrid frequency-hopping pseudonoise systems		

DD FORM 1 JAN 73 1073 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

1 SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

410741 Lu

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

ABSTRACT (Cont'd)

are discussed. Differences in the error rate performance between frequency-hopping systems and pseudonoise systems are illustrated.

Accession For	
NTIS GRA&I	<input checked="checked" type="checkbox"/>
DDC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Dissemination /	
Availability /	
Dist	Availability for Special
A	

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

## **.CONTENTS**

	<u>Page</u>
1. PRINCIPLES .....	5
2. CONCEALMENT OF PSEUDONOISE WAVEFORMS .....	8
3. ERROR PROBABILITIES IN PRESENCE OF INTERFERENCE .....	11
4. PSEUDONOISE NETWORKS .....	15
5. JAMMING .....	16
6. CODE SYNCHRONIZATION .....	16
7. HYBRID SYSTEM .....	18
8. COMPARISON WITH FREQUENCY HOPPING .....	19
9. CONCLUSIONS .....	20
LITERATURE CITED .....	21
GLOSSARY OF PRINCIPAL SYMBOLS .....	23
DISTRIBUTION .....	25

## **FIGURES**

1. Generic spread-spectrum system .....	5
2. Generic form of pseudonoise system transmitter with biphase and quadriphase-shift keying for spectrum spreading .....	5
3. Direct-sequence pseudonoise system .....	6
4. Spectra of desired signal and interference .....	6
5. Quadriphase pseudonoise system .....	7
6. Pseudonoise system with binary code-shift keying .....	7
7. Autocorrelation of linear maximal sequence .....	8
8. Power spectral density of pseudorandom code .....	9
9. Basic elements of ideal receiver for pseudonoise system .....	11

## CONTENTS (Cont'd)

10. Comparison of uncoded and coded word error probabilities in presence of optimal interference .....	14
11. Time-hopping pseudonoise system .....	16
12. Serial acquisition system .....	17
13. Matched-filter acquisition system with protection against interference .....	18
14. Hybrid frequency-hopping pseudonoise system .....	19
15. Comparison of uncoded word error probabilities for pseudonoise and frequency hopping in presence of narrowband jamming at center frequency .....	19
16. Comparison of coded word error probabilities for pseudonoise and frequency hopping in presence of narrowband jamming at center frequency .....	20



## 1. PRINCIPLES

Spread-spectrum modulation is a modulation that produces a signal with a bandwidth much wider than the message bandwidth. Because a spread-spectrum system distributes the transmitted energy over a wide bandwidth, the signal-to-noise ratio at the receiver input is low. Nevertheless, the receiver is capable of operating successfully because the transmitted signal has distinct characteristics relative to other signals such as interference or environmental noise. The generic forms of the transmitter and the receiver in a spread-spectrum system are shown in figure 1.

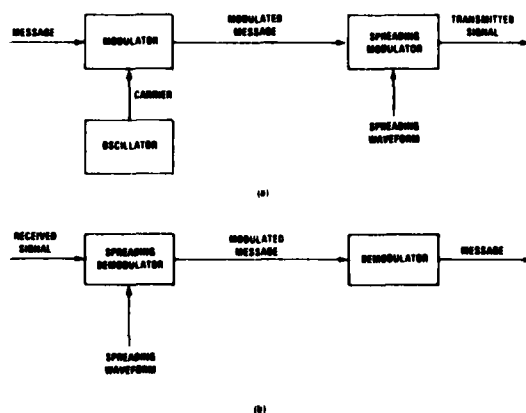


Figure 1. Generic spread-spectrum system:  
(a) transmitter and (b) receiver.

The spreading waveform is controlled by a pseudonoise code, which is a binary sequence that is apparently random, but can be reproduced deterministically by intended users. The pseudonoise code gives spread-spectrum systems identification and selective calling capabilities.

Spread-spectrum systems<sup>1,3</sup> are useful for military communications because they make it difficult

<sup>1</sup>R. C. Dixon, *Spread Spectrum Systems*, John Wiley and Sons, Inc., New York (1976).

<sup>2</sup>*Spread Spectrum Communications*, NATO Advisory Group for Aerospace Research and Development, National Technical Information Service AD766914 (1973).

<sup>3</sup>M. G. Unkuf, in *Surface Wave Filters*, H. Matthews, ed., John Wiley and Sons, Inc., New York (1977).

to detect the transmitted waveform, extract the message, or jam the intended receiver. Constraints such as those on transmitter peak power and linearity limit the variety of practical spread-spectrum systems. The most widely used spread-spectrum methods are pseudonoise modulation, frequency hopping, and hybrids of these two methods. In this report, we examine the most important aspects of pseudonoise spread-spectrum systems with respect to military communications.

Pseudonoise spread-spectrum systems usually accomplish the spectrum spreading by phase modulation. Figure 2 shows the generic form of the transmitter in a pseudonoise system with binary phase-shift keying or quadriphase-shift keying for spectrum spreading.

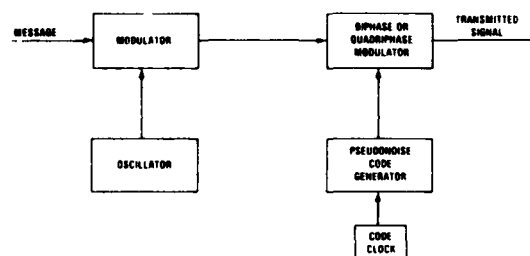


Figure 2. Generic form of pseudonoise system transmitter with biphase and quadriphase-shift keying for spectrum spreading.

Message privacy is provided by a spread-spectrum system if a transmitted message cannot be recovered without knowledge of the pseudonoise code. If message privacy is required, most analog message modulations cannot be used since the pseudonoise code transitions provide a possible basis for separating the code from the message. If the message is in digital form but the data bits are asynchronous with the code clock, the data bit transitions do not coincide with the pseudonoise code transitions and separation is possible. Thus, message privacy requires synchronization of the data bit transitions with the code clock. This synchronization may be accomplished by either feeding the code clock back to the data source, if feasible, or providing for bit storage. Since the data

and the code are synchronized at the transmitter, code synchronization in the receiver automatically gives data bit synchronization.

Figure 3 is a functional block diagram of a pseudonoise system with message privacy. This implementation of spread-spectrum modulation, often called direct-sequence modulation, is the most widely used implementation in practice. Synchronized data bits and pseudonoise code bits, which are called chips, are modulo-two added before the binary phase-shift keying (PSK). A coherent PSK demodulator may be used in the receiver. Alternatively, if differential encoding and detection of the data bits are desired, a differential phase-shift keying demodulator is used in the receiver.

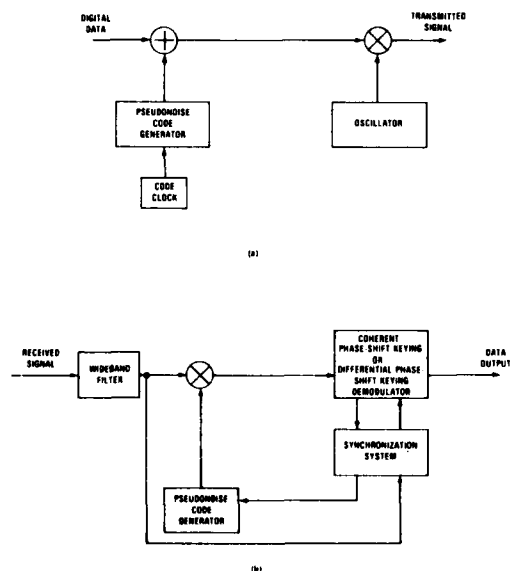


Figure 3. Direct-sequence pseudonoise system: (a) transmitter and (b) receiver.

The received signal can be represented by

$$s(t) = Am(t)p(t) \cos(\omega_0 t + \theta) \quad (1)$$

where  $A$  is the amplitude,  $m(t)$  is the binary message sequence,  $p(t)$  is the binary pseudonoise code sequence,  $\omega_0$  is the carrier frequency,

and  $\theta$  is the phase angle. Both  $m(t)$  and  $p(t)$  take the value  $+1$  or  $-1$ . The message bits have a duration of  $T_m$ , and the chips have a shorter duration of  $T_p$ . Since the message bit and chip transitions coincide on both sides of a message bit, the ratio of  $T_m$  to  $T_p$  is an integer. If  $B_p$  is the bandwidth of  $s(t)$  and  $B_m$  is the bandwidth of  $m(t) \cos \omega_0 t$ , the spectrum spreading due to  $p(t)$  gives  $B_p \gg B_m$ .

At the communication receiver, demodulation proceeds as indicated in figure 3(b). We ignore possible synchronization problems. After passage through the wideband filter of bandwidth  $B_p$ , the signal is multiplied by a local code replica of  $p(t)$ . Since  $p^2(t) = 1$ , this multiplication yields

$$s_1(t) = Am(t) \cos(\omega_0 t + \theta)$$

at the input of the demodulator. Since  $s_1(t)$  has the form of a PSK signal, the corresponding demodulation extracts  $m(t)$ .

The action of the receiver in reducing interference is qualitatively illustrated in figure 4; quantitative results are given subsequently. Figure 4(a) shows the relative spectra of the desired signal and interference at the output of the wideband filter. Multiplication by the pseudonoise code produces the spectra of figure 4(b) at the demodulator input. The signal bandwidth is reduced to  $B_m$  while the interference energy is spread over a bandwidth exceeding  $B_p$ . The filtering action of the demodula-

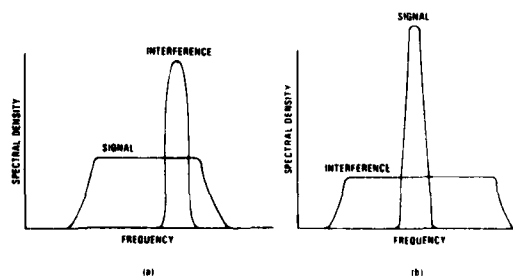


Figure 4. Spectra of desired signal and interference: (a) wideband filter output and (b) demodulator input.

tor removes most of the interference spectrum that does not overlap the signal spectrum. Thus, most of the original interference energy is eliminated and does not affect the receiver performance. The ratio  $B_p/B_m$ , which is called the processing gain, is a measure of the interference rejection.

Two other pseudonoise systems with potential message privacy are diagrammed in figures 5 and 6. We discuss these systems briefly and then restrict attention to the direct-sequence systems. For simplicity, figures 5 and 6 omit depictions of the synchronization systems.

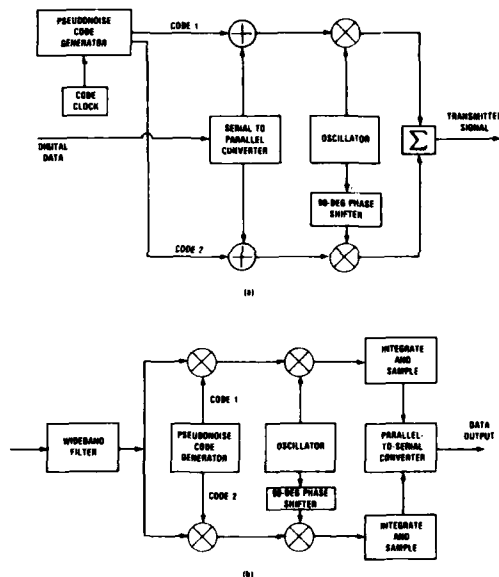


Figure 5. Quadriphase pseudonoise system: (a) transmitter and (b) receiver.

Figure 5 shows a pseudonoise system with quadriphase-shift keying. Two pseudonoise codes, which may be derived from a single generator, are used with two quadrature carriers. Each member of each successive pair of data bits is combined with one of the pseudonoise codes and one of the quadrature carriers. In each branch of the receiver, one of the codes is removed, followed by coherent PSK demodulation. The output bits of the two branches are alternately sampled to reconstruct the data stream.

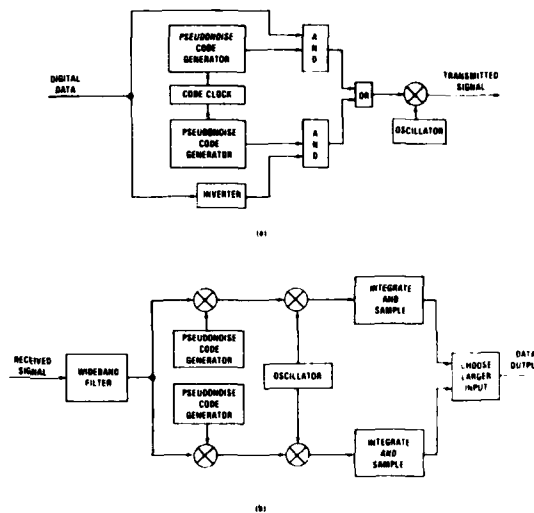


Figure 6. Pseudonoise system with binary code-shift keying: (a) transmitter and (b) receiver.

Figure 6 shows a pseudonoise system with binary code-shift keying. Depending upon the logical state of the digital data, one or the other of two nearly orthogonal pseudonoise codes is transmitted. In the receiver, each code creates a significant output in only one of the two parallel branches. Thus, the data are recovered by comparing the branch outputs. In a pseudonoise system with  $M$ -ary code-shift keying, each group of  $n$  data bits is encoded as one of  $M = 2^n$  codes chosen to have small cross correlations. The main advantage of this system is its relative insensitivity to an unintentional frequency offset in the carrier. However, binary code-shift keying systems exhibit a relatively poor bit error probability in white Gaussian noise, whereas  $M$ -ary systems have improved bit error probabilities, but require complex implementations.<sup>3</sup>

The autocorrelation of a periodic function,  $x(t)$ , with period  $T_x$  is defined as

<sup>3</sup>M. G. Unkauf, in *Surface Wave Filters*, H. Matthews, ed., John Wiley and Sons, Inc., New York (1977).

$$R_x(\tau) = \frac{1}{T_x} \int_{-T_x/2}^{T_x/2} x(t)x(t + \tau) dt \quad , \quad (2)$$

where  $\tau$  is the relative delay variable. The autocorrelation is periodic with period  $T_x$ . The pseudonoise codes are usually linear maximal sequences generated by feedback shift registers. If the code length before repetition is  $K$  chips and the duration of a chip is  $T_p$ , the code period is  $KT_p$ . Using equation (2), we can derive the autocorrelation of a unit-amplitude linear maximal sequence,  $p(t)$ . Over the interval

$$|\tau| \leq KT_p/2 \quad ,$$

we obtain<sup>4</sup>

$$R_p(\tau) = \begin{cases} 1 - \left(\frac{K+1}{K}\right) \frac{|\tau|}{T_p} & , |\tau| \leq T_p \\ -\frac{1}{K} & , |\tau| > T_p \end{cases} \quad (3)$$

Since  $R_p(\tau)$  is periodic with period  $KT_p$ , it is completely specified by equation (3). This function is plotted in figure 7.

The autocorrelation is sharply peaked for zero delay, but relatively small for other delays. Consequently, the linear maximal sequences are desirable for code synchronization in the receiver. Nonlinear sequences and linear nonmaximal sequences often exhibit minor peaks in their auto-

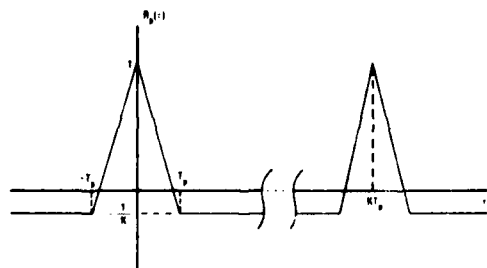


Figure 7. Autocorrelation of linear maximal sequence.

<sup>4</sup>W. C. Lindsey and M. K. Simon, *Telecommunication Systems Engineering*, Prentice-Hall, Inc., Englewood Cliffs, NJ (1973).

correlation functions. These minor peaks hinder rapid code synchronization.

The triangular autocorrelation enables the receiver to discriminate against delayed signal replicas caused by multipath effects. Thus, if the multipath delay exceeds  $T_p$ , the resulting receiver performance degradation is usually negligible.

Linear pseudonoise codes are inherently susceptible to mathematical cryptanalysis. Thus, if message security is desired, the message may be enciphered before it is added to the pseudonoise code for spectrum spreading.

Although cryptographic integrity may be lacking, long pseudonoise codes make it more difficult for hostile personnel to deduce the code and produce effective jamming or to extract an unenciphered message from intercepted pseudonoise communications. However, long codes increase the time needed for synchronization at the receiver.

## 2. CONCEALMENT OF PSEUDONOISE WAVEFORMS

In this section, we derive the conditions under which the transmitted output of a pseudonoise system is difficult to detect by a simple spectrum analyzer. To write a compact equation for  $R_p(\tau)$ , it is convenient to use the following notation for a triangular pulse:

$$\Lambda\left(\frac{t}{T}\right) = \begin{cases} 1 - \frac{|t|}{T} & , t \leq T \\ 0 & , t > T \end{cases} \quad (4)$$

We then may write

$$R_p(\tau) = -\frac{1}{K} + \frac{K+1}{K} \sum_{i=-\infty}^{\infty} \Lambda\left(\frac{t - iKT_p}{T_p}\right) \quad (5)$$

The Fourier transform of a function  $x(t)$  is defined by

$$F\{x(t)\} = \int_{-\infty}^{\infty} x(t)e^{-j2\pi ft} dt, \quad (6)$$

where  $f$  is the frequency variable and  $j = \sqrt{-1}$ . A straightforward calculation or Fourier transform tables give

$$F\left\{\Lambda\left(\frac{t}{T}\right)\right\} = T \operatorname{sinc}^2 fT, \quad (7)$$

where it is convenient to define

$$\operatorname{sinc} x = \frac{\sin \pi x}{\pi x}. \quad (8)$$

The summation on the right side of equation (5) is a periodic function with period  $T_p$ . Thus, it can be expressed as a complex exponential Fourier series. We take the Fourier transform of this series, express the Fourier coefficients as Fourier transforms, and use equation (7). The result is

$$\begin{aligned} & F\left\{\sum_{i=-\infty}^{\infty} \Lambda\left(\frac{t - iKT_p}{T_p}\right)\right\} \\ &= \frac{1}{K} \sum_{i=-\infty}^{\infty} \operatorname{sinc}^2\left(\frac{i}{K}\right) \delta\left(f - \frac{i}{KT_p}\right), \quad (9) \end{aligned}$$

where  $\delta(\cdot)$  is the Dirac delta function. We use the preceding results to determine  $S_p(f)$ , the power spectral density of  $p(t)$ , which is defined as the Fourier transform of  $R_p(\tau)$ . Taking the Fourier transform of equation (5), substituting equation (9), noting that the Fourier transform of a constant is a delta function, and rearranging the result, we obtain

$$\begin{aligned} S_p(f) &= \frac{K+1}{K^2} \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \operatorname{sinc}^2\left(\frac{i}{K}\right) \\ &\times \delta\left(f - \frac{i}{KT_p}\right) + \frac{1}{K^2} \delta(f). \quad (10) \end{aligned}$$

This function is plotted in figure 8. It consists of delta functions separated by  $1/KT_p$ .

The autocorrelation of a stochastic process,  $x(t)$ , is defined by

$$R_x(t, \tau) = E[x(t)x(t + \tau)] \quad (11)$$

where  $E[y]$  is the expected value of  $y$ . If  $x(t)$  is a stationary process, then  $R_x(t, \tau)$  is a function of  $\tau$  alone, and we denote the autocorrelation by  $R_x(\tau)$ . The power spectral density of a stationary process is defined as the Fourier transform of its autocorrelation. For a nonstationary process, a time-average power spectral density can be defined. First, we define the average autocorrelation of  $x(t)$  as

$$\bar{R}_x(\tau) = \lim_{T \rightarrow \infty} \frac{1}{2T} \int_{-T}^T R_x(t, \tau) dt \quad (12)$$

The limit exists and is not identically zero if  $x(t)$  has finite power and infinite duration. If  $x(t)$  is stationary,  $\bar{R}_x(\tau) = R_x(\tau)$ . The average power spectral density, denoted by  $\bar{S}_x(f)$ , is defined as the Fourier transform of the average autocorrelation.

We assume that the message,  $m(t)$ , is a stationary stochastic process with an autocorrelation of  $R_m(\tau)$ . We assume that  $\theta$  in equation (1) is a random variable uniformly distributed over the interval  $[0, 2\pi]$  and statistically independent of  $m(t)$ . The autocorrelation of

$$m_i(t) = m(t) \cos(\omega_0 t + \theta)$$

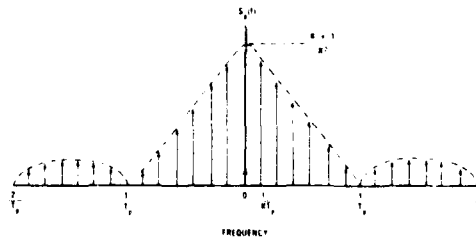


Figure 8. Power spectral density of pseudo-random code.

is determined by applying equation (11) and using trigonometry. The result is independent of  $t$ , so we write

$$R_{m1}(\tau) = \frac{1}{2} R_m(\tau) \cos \omega_0 \tau \quad (13)$$

Thus, the power spectral density of  $m_1(t)$  is

$$S_{m1}(f) = \frac{1}{4} [S_m(f - f_0) + S_m(f + f_0)] \quad (14)$$

where  $f_0 = \omega_0/2\pi$  and  $S_m(f)$  is the power spectral density of  $m(t)$ .

By using equations (1) and (11) and noting that  $p(t)$  is deterministic, the autocorrelation of  $s(t)$  is determined to be

$$R_s(t, \tau) = A^2 p(t)p(t + \tau)R_{m1}(\tau) \quad (15)$$

which indicates that  $s(t)$  is a nonstationary process. Since  $p(t)$  is periodic, the definitions of equations (2) and (12) yield

$$\bar{R}_s(\tau) = A^2 R_p(\tau)R_{m1}(\tau) \quad (16)$$

Consequently,  $\bar{S}_s(f)$ , the average power spectral density of  $s(t)$ , is the convolution of  $A^2 S_p(f)$  with  $S_{m1}(f)$ . Using equation (10), we get

$$\begin{aligned} \bar{S}_s(f) &= A^2 \frac{K+1}{K^2} \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \text{sinc}^2 \left( \frac{i}{K} \right) \\ &\times S_{m1} \left( f - \frac{i}{KT_p} \right) + \frac{A^2}{K^2} S_{m1}(f) \quad (17) \end{aligned}$$

Substituting equation (14), we obtain

$$\begin{aligned} \bar{S}_s(f) &= \frac{A^2}{4K^2} S_m(f - f_0) + A^2 \frac{K+1}{4K^2} \\ &\times \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \text{sinc}^2 \left( \frac{i}{K} \right) S_m \left( f - f_0 - \frac{i}{KT_p} \right) \\ &+ \frac{A^2}{4K^2} S_m(f + f_0) + A^2 \frac{K+1}{4K^2} \end{aligned}$$

$$\times \sum_{\substack{i=-\infty \\ i \neq 0}}^{\infty} \text{sinc}^2 \left( \frac{i}{K} \right) S_m \left( f + f_0 + \frac{i}{KT_p} \right) \quad (18)$$

This equation gives the average power spectrum of a transmitted signal in a pseudonoise communication system.

If a transmission has a low power spectral density compared with thermal and environmental noise and if the spectrum is uniform, then it is difficult to detect the presence of the signal with a simple spectrum analyzer. To ensure that the spectrum is flat, the spectral contributions of the terms in the summations of equation (18) must overlap. The center of the spectral contribution of a term is separated from the center of the spectral contribution of an adjacent term by  $1/KT_p$ . Thus,  $B_m \geq 2/KT_p$  is required if  $\bar{S}_s(f)$  is to be approximately flat. Since  $B_p \approx 2/T_p$ , an approximate necessary condition for communication concealment from spectrum analysis is

$$K \geq \frac{B_p}{B_m} \quad (19)$$

that is, the code length must exceed the processing gain.

Since messages tend to be nearly random in character, it is plausible to model  $m(t)$  as a random binary sequence. This stationary process has a mean value of zero. The autocorrelation of a random binary sequence of bit period  $T_m$  is<sup>5</sup>

$$R_m(\tau) = \Lambda \left( \frac{\tau}{T_m} \right) \quad (20)$$

Equation (7) gives the corresponding power spectral density:

$$S_m(f) = T_m \text{sinc}^2 f T_m \quad (21)$$

The associated bandwidth is  $B_m \approx 2/T_m$ . Thus, an alternative necessary condition for concealment is

$$KT_p \geq T_m \quad (22)$$

<sup>5</sup>S. Haykin, *Communication Systems*, John Wiley and Sons, Inc., New York (1978).

which simply states that the pseudonoise code period must equal or exceed a data bit duration.

The fact that a pseudonoise signal is concealed does not mean that it cannot be detected. Suppose that  $s(t)$  enters a wideband receiver and is squared. Since  $m^2(t) = p^2(t) = 1$ , the output of the squaring device is proportional to

$$\begin{aligned} s^2(t) &= A^2 \cos^2(\omega_0 t + \theta) \\ &= \frac{A^2}{2} + \frac{A^2}{2} \cos(2\omega_0 t + 2\theta) \end{aligned} \quad (23)$$

If  $s^2(t)$  is applied to an integrator or a narrowband filter, the energy of the signal can often be detected, even if  $\bar{S}_s(f)$  is far below the noise power spectral density.<sup>6</sup> The double-frequency term of equation (23) can be applied to a separate filter for estimation of the carrier frequency,  $f_0$ , of the pseudonoise signal. Although detection and frequency might be estimated in this manner, an interceptor cannot demodulate  $s(t)$  without knowledge of  $p(t)$ .

### 3. ERROR PROBABILITIES IN PRESENCE OF INTERFERENCE

The bit error probability of an ideal coherent PSK system operating in zero-mean, white Gaussian noise is<sup>7</sup>

$$P_b = \frac{1}{2} \operatorname{erfc} \left[ \left( \frac{E_b}{N_0} \right)^{1/2} \right] \quad (24)$$

where the complementary error function is defined by

$$\operatorname{erfc} x = \frac{2}{\sqrt{\pi}} \int_x^\infty \exp(-y^2) dy \quad (25)$$

$E_b$  is the energy per bit, and  $N_0/2$  is the noise power spectral density. The PSK demodulator can be modeled as a matched filter, sampler, and threshold device as shown in figure 9. Suppose that

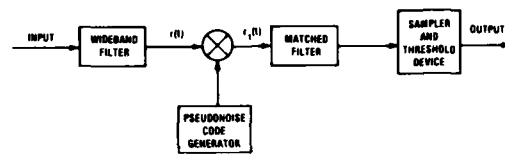


Figure 9. Basic elements of ideal receiver for pseudonoise system.

interference, which may be jamming, accompanies the desired signal at the receiver. After passage through the wideband filter, the total received signal is

$$r(t) = s(t) + j(t) + n(t) \quad (26)$$

where  $j(t)$  represents the interference and  $n(t)$  represents the thermal noise. From equation (1), the input to the matched filter is

$$r_1(t) = A m(t) \cos(\omega_0 t + \theta) + i(t) \quad (27)$$

where

$$i(t) = j(t)p(t) + n(t)p(t) \quad (28)$$

is the total interference entering this filter. The factor  $p(t)$  in this equation ensures that the energy in  $i(t)$  is spread over a bandwidth at least equal to  $B_p$ . It is possible to use equation (24) to determine an approximate formula for the bit error probability of a pseudonoise system by substituting  $S_i(f)$ , the power spectral density of  $i(t)$ , for  $N_0/2$  in this equation. The derivation of equation (24) indicates that this approach is legitimate if (1)  $i(t)$  is a zero-mean, stationary process; (2) the interference emerging from the matched filter,  $i_1(t)$ , is a Gaussian random variable at the sampling times; (3)  $S_i(f)$  is approximately flat over the bandwidth of the matched filter,  $B_m$ .

To satisfy these three requirements, we make several assumptions that are intuitively plausible. We assume that  $j(t)$  and  $n(t)$  are stationary stochastic processes that are statistically independent of each other and  $p(t)$ . We assume that  $KT_p \gg T_m$  so that during a message bit interval  $p(t)$  is well approximated as a random binary sequence. It follows that  $i(t)$  is a zero-mean, stationary process. In view of the central limit

<sup>6</sup>D. J. Torrieri, *Interception of Hostile Communications*, U.S. Army Materiel Development and Readiness Command CM/CCM-79-3 (October 1979).

<sup>7</sup>R. E. Ziemer and W. H. Tranter, *Principles of Communications*, Houghton-Mifflin Co., Boston (1976).

theorem and the fact that the filtering operation can be approximated as a summation, it is reasonable to assume that  $i_1(t)$  is approximately a Gaussian random variable at the sampling time. Thus, the first two requirements are approximately satisfied.

Since  $j(t)$ ,  $n(t)$ , and  $p(t)$  are statistically independent, the autocorrelation of  $i(t)$  is

$$R_i(\tau) = R_j(\tau)R_p(\tau) + R_n(\tau)R_p(\tau) \quad (29)$$

Since  $p(t)$  is approximated by a random binary sequence, its autocorrelation and power spectral density are

$$R_p(\tau) = \Lambda\left(\frac{\tau}{T_p}\right), \quad (30)$$

$$S_p(f) = T_p \operatorname{sinc}^2 f T_p.$$

We approximate  $n(t)$  by white Gaussian noise so that its autocorrelation and power spectral density are

$$R_n(\tau) = \delta(\tau), \quad (31)$$

$$S_n(f) = \frac{N_0}{2}.$$

Taking the Fourier transform of  $R_i(\tau)$  and using equations (30) and (31) and the convolution theorem, we obtain the power spectral density of the interference,

$$S_i(f) = \frac{N_0}{2} + T_p \times \int_{-\infty}^{\infty} \operatorname{sinc}^2 [(f - u)T_p] S_j(u) du \quad (32)$$

The matched filter has a center frequency of  $f_0$  and a bandwidth of  $B_m$ . For practical pseudonoise systems,  $B_m \ll B_p$ . Thus,  $B_m T_p \ll 1$ , and  $S_i(f)$  is approximately flat over the matched filter bandwidth.

We assume that  $f_0 T_p$  is sufficiently large for  $\operatorname{sinc}^2(x)$  to be negligible for  $x \geq f_0 T_p$ . Since  $j(t)$  is the output of a wideband filter of bandwidth  $B_p$ , we have the following approximation:

$$S_i(f_0) \approx \frac{N_0}{2} + T_p \times \int_{f_0 - B_p/2}^{f_0 + B_p/2} \operatorname{sinc}^2 [(f_0 - u)T_p] S_j(u) du \quad (33)$$

Since the three requirements for using equation (24) are satisfied, we substitute  $S_i(f_0)$  for  $N_0/2$  in equation (24) to determine the bit error probability of a pseudonoise system.

Several special cases are of particular interest. Suppose  $j(t)$  has power  $R_j$  and a flat spectrum over  $B_p$  so that  $S_j(u) = R_j/2B_p$  in equation (33). Then

$$S_i(f_0) \approx \frac{N_0}{2} + \frac{b R_j T_p}{2}, \quad (34)$$

where we define

$$b = \frac{1}{B_p} \int_{f_0 - B_p/2}^{f_0 + B_p/2} \operatorname{sinc}^2 [(f_0 - u)T_p] du \quad (35)$$

Since  $\operatorname{sinc}(x) \leq 1$ , we have  $b \leq 1$ .

Next, suppose that  $j(t) = A_1 \cos(\omega_1 t + \phi)$ , where  $A_1$  is the amplitude, carrier frequency  $f_1 = \omega_1/2\pi$  is within the bandwidth of the wideband filter, and  $\phi$  is a uniformly distributed random variable. The power in  $j(t)$  is  $R_j = A_1^2/2$ . A straightforward calculation gives

$$S_j(f) = \frac{R_j}{2} [\delta(f - f_1) + \delta(f + f_1)] \quad (36)$$

Equations (33) and (36) yield

$$S_i(f_0) \approx \frac{N_0}{2} + \frac{R_j T_p}{2} \operatorname{sinc}^2 [(f_0 - f_1)T_p] \quad (37)$$

Equation (37) can be written in the form of equation (34). For center-frequency, tone (unmodulated-carrier) interference, we have  $b = 1$ . When narrowband interference that is offset from the receiver center frequency is present, we have  $b < 1$ . More precisely,

$$b = \operatorname{sinc}^2 [(f_0 - f_1)T_p] \quad (38)$$

A third special case occurs when  $j(t)$  has the form



$$j(t) = A_1 q(t) \cos(\omega_1 t + \phi) \quad (39)$$

where  $q(t)$  is an interfering pseudonoise sequence. If the cross correlation of  $p(t)$  and  $q(t)$  is small for all relative delays and  $q(t)$  has a long period compared with  $T_m$ , it is reasonable to model  $q(t)$  as an independent binary random sequence. The autocorrelation of  $j(t)p(t)$  is

$$R_{jp}(\tau) = R_j R_p(\tau) R_q(\tau) \cos \omega_1 \tau \quad (40)$$

where  $R_j = A_1^2/2$  is the power in  $j(t)$ . The autocorrelation of  $R_p(\tau)$  is given in equation (30). The autocorrelation of  $q(t)$  is

$$R_q(\tau) = \Lambda\left(\frac{\tau}{T_q}\right) \quad (41)$$

where  $T_q$  is the bit duration of the sequence  $q(t)$ . By using equations (30), (40), and (41), the power spectral density of  $R_{jp}(\tau)$  can be written as

$$S_{jp}(f) = R_j \int_{-T_0}^{+T_0} \Lambda\left(\frac{\tau}{T_p}\right) \Lambda\left(\frac{\tau}{T_q}\right) \times \cos 2\pi f_1 \tau \cos 2\pi f \tau d\tau \quad (42)$$

where

$$T_0 = \min(T_p, T_q) \quad (43)$$

Simple trigonometry transforms equation (42) into two integrals. If we assume that  $f_0 - f_1 \ll f_0 + f_1$  and  $(f_0 + f_1)T_0 \gg 1$ , only one of the integrals contributes significantly to  $S_{jp}(f_0)$ . Thus,

$$S_{jp}(f_0) \approx R_j \int_0^{T_0} \Lambda\left(\frac{\tau}{T_p}\right) \Lambda\left(\frac{\tau}{T_q}\right) \times \cos [2\pi(f_0 - f_1)\tau] d\tau \quad (44)$$

This integral can be evaluated by using the algebraic expressions for the functions and standard integrals. For  $T_0 \neq 0$ , we obtain

$$S_{jp}(f_0) = R_j \left\{ \frac{\cos [2\pi(f_0 - f_1)T_0]}{(2\pi)^2 (f_0 - f_1)^2} \left( \frac{1}{T_1} - \frac{1}{T_0} \right) - \frac{2 \sin [2\pi(f_0 - f_1)T_0]}{(2\pi)^3 (f_0 - f_1)^3 T_1 T_0} \right.$$

$$\left. + \frac{1}{(2\pi)^2 (f_0 - f_1)^2} \left( \frac{1}{T_1} + \frac{1}{T_0} \right) \right\}, \quad f_0 \neq f_1 \quad (45)$$

where we have defined

$$T_1 = \max(T_p, T_q) \quad (46)$$

If  $f_0 = f_1$ , we obtain

$$S_{jp}(f_0) \approx R_j \left( \frac{T_0}{2} - \frac{T_0^2}{6T_1} \right), \quad f_0 = f_1 \quad (47)$$

If  $T_p = T_q$ , equations (45) and (47) become

$$S_{jp}(f_0) = \frac{R_j}{2\pi^2 (f_0 - f_1)^2 T_p} \times \{1 - \text{sinc}[2(f_0 - f_1)T_p]\} \quad T_p = T_q, f_0 \neq f_1 \quad (48)$$

$$S_{jp}(f_0) = \frac{R_j T_p}{3}, \quad T_p = T_q, f_0 = f_1$$

The power spectral density of  $i(t)$  is

$$S_i(f_0) = \frac{N_0}{2} + S_{jp}(f_0) \quad (49)$$

With  $b = 2S_{jp}(f_0)/R_j T_p$ , this equation can be written in the form of equation (34). Thus, for pseudonoise interference and  $f_0 = f_1$ , we have

$$b = \frac{T_0}{T_p} \left( 1 - \frac{T_0}{3T_1} \right), \quad f_0 = f_1 \quad (50)$$

This equation indicates that  $b$  increases with increasing  $T_q$  if  $f_0 = f_1$ . If  $T_p = T_q$ , we have

$$b = \frac{2}{3}, \quad T_p = T_q, f_0 = f_1 \quad (51)$$

Equation (44) indicates that the power spectral density and, hence,  $b$  are greatest when  $f_1 = f_0$ . Given that  $f_1 = f_0$ , equation (50) indicates that  $b \leq 1$ . Thus, in all three special cases of  $j(t)$ , we have  $b \leq 1$ . We call  $b$  the interference parameter. It is a measure of the effectiveness of an

interference type relative to optimal tone interference.

If more than one statistically independent source of interference is present, equation (34) can still be used. Assuming that all types of interference are similar to the three special cases considered, the linearity of the demodulation allows calculation of the appropriate value of  $b$ . If  $R_j$  is interpreted as the total interference power,

$$b = \frac{1}{R_j} \sum_i b_i R_{ji} \quad (52)$$

where  $R_{ji}$  is the interference power due to source  $i$  and  $b_i$  is the corresponding interference parameter. Since the  $b_i \leq 1$ , we still have  $b \leq 1$ .

The energy per bit may be expressed as  $E_b = R_s T_m$ , where  $R_s$  is the average power in the intended transmission. Replacing  $N_0/2$  in equation (24) by the right side of equation (34) yields the bit error probability for an ideal coherent pseudonoise system. Rearranging the result gives

$$P_b = \frac{1}{2} \operatorname{erfc} \left[ \left( \frac{b R_j}{G R_s} + \frac{N_0}{E_b} \right)^{1/2} \right] \quad (53)$$

where

$$G = \frac{B_p}{B_m} = \frac{T_m}{T_p} \quad (54)$$

is the processing gain. Other calculations of the bit error probability for various conditions can be found in the literature.<sup>8</sup>

Increasing the processing gain is helpful against interference for which  $R_j$  is fixed. Increasing the processing gain by increasing  $B_p$  is not helpful against interference for which  $R_j$  increases proportionately with  $B_p$ .

Suppose words of  $w$  data bits are block encoded so that  $c$  bits are transmitted for each word. Depending upon the code,  $r$  or more bits

per code word must be in error for a word error to occur at the receiver output. Assuming that bit errors occur independently, the probability of a word error is

$$P_w = \sum_{m=r}^c \binom{c}{m} (1 - P_c)^{c-m} P_c^m \quad (55)$$

where  $P_c$  is the probability of an error in an encoded bit. If the duration of a word is preserved after encoding, the duration of an encoded bit is  $T_m' = w T_m / c$ . Thus, the energy per encoded bit is  $E_b' = w E_b / c$ , and the processing gain becomes  $G' = w G / c$ . By analogy with equation (53), we obtain

$$P_c = \frac{1}{2} \operatorname{erfc} \left[ \left( \frac{c b R_j}{w G R_s} + \frac{c N_0}{w E_b} \right)^{1/2} \right] \quad (56)$$

When the total bandwidth and the word duration are fixed, the potential improvement in performance due to encoding is partially counterbalanced by the decrease in processing gain, which results from the increased transmitted bit rate. As an illustration, let  $b = 1$  and  $G = 1000$  (30 dB). Figure 10 shows  $P_w$  as a function of the signal-to-noise ratio per word,  $c E_b' / N_0 = w E_b / N_0$ , for uncoded words with  $c = w = 4$  and  $r = 1$  and for coded words with  $c = 7$ ,  $w = 4$ , and  $r = 2$ . The interference-to-signal ratio,  $R_j / R_s$ , is 10 dB for one pair of curves and 20 dB for the other.

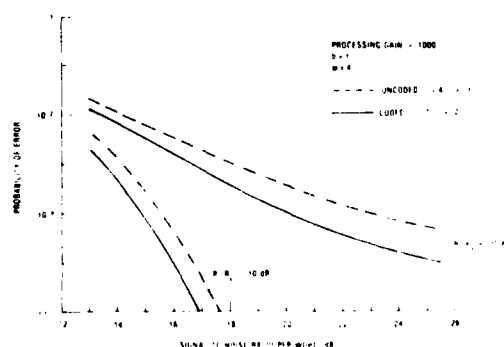


Figure 10. Comparison of uncoded and coded word error probabilities in presence of optimal interference;  $b$  = interference parameter,  $w$  = number of data bits,  $c$  = number of code bits,  $r$  = number of bit errors required for word error.

<sup>8</sup>Special Issue on Spread Spectrum Communications, IEEE Trans. Comm., Com-25 (August 1977).

It has been assumed that the interference is a stationary process. If the interference is sporadic with high power, such as occurs during pulsed jamming, then bit interleaving after encoding and before transmission may be useful. After deinterleaving at the receiver, a burst of errors is spread over a number of different words. The error correction decoding may then remove the errors.

#### 4. PSEUDONOISE NETWORKS

A pseudonoise network is a communication network in which each element is a pseudonoise system controlled by a different code. The elements cause mutual interference, which increases the bit error probability in a receiver. We can minimize the increase and use the results of the analysis following equation (39) if the cross correlations between the various pseudonoise codes are small and the code periods are long compared with  $T_m$ . For practical reasons, all network elements usually have common carrier frequencies and chip rates. If the network elements have different code lengths, cross correlations are usually small if the code lengths do not contain common factors. If, for practical reasons, all network elements have a common code length, it is usually desirable in finding maximal code sets with small cross correlations to choose a code length that does not have small factors; there exist large families of nonmaximal codes with bounded cross correlations.

Assuming that the cross correlations are negligible and the code periods are much longer than  $T_m$ , we can use equation (53) to calculate  $P_b$  in the presence of mutual interference. To minimize the parameter  $b$ , the network elements should have different carrier frequencies and different chip rates whenever practical.

One method of counteracting mutual interference is to use time division multiplexing. If there are  $N$  elements in the network, each element is assigned a separate time slot for transmission during each interval of duration  $T_n$ . Neglecting propagation time uncertainties, this procedure eliminates the mutual interference, but requires that the transmitted data bit rate be increased by the factor  $N$  or more during the allotted time slots if

the overall data bit rate is to remain constant. If the transmitted bits have duration  $T_m/N$  in a network with time division multiplexing, the bit error probability in the absence of mutual interference (and other interference) is

$$P_b = \frac{1}{2} \operatorname{erfc} \left[ \left( \frac{R_s T_m}{NN_0} \right)^{1/2} \right] \quad (57)$$

where  $R_s$  is the received signal power from a transmitter during one of its time slots. If the transmitters of the pseudonoise systems are not peak-power limited, then  $R_s = NR_s$  preserves the average transmitted power over  $T_n$ . In this case, a comparison of equations (57) and (53) for  $E_b = R_s T_m$  indicates that the time division multiplexing is always helpful. If the transmitters are peak-power limited, time division multiplexing is helpful if

$$N < \frac{R_s}{R_i} \left( 1 + \frac{bR_i T_p}{N_0} \right) \quad (58)$$

where  $R_i$  is the power due to interference from the other network elements. If the elements have a common chip rate and carrier frequency, then  $b = 2/3$ .

Time-division multiplexing requires coordination among the network elements. If coordination is not feasible, the various time slots of the elements may overlap with each other, causing mutual interference. Nevertheless, the interference power at a receiver is reduced to an average on the order of  $R_i = R_i/N$ . The processing gain becomes  $G = G/N$ . Thus, the bit error probability is approximately

$$P_b = \frac{1}{2} \operatorname{erfc} \left[ \left( \frac{bR_i}{GR_s} + \frac{NN_0}{R_s T_m} \right)^{1/2} \right] \quad (59)$$

If the transmitters of the pseudonoise systems are not peak-power limited, so that  $R_s = NR_s$ , the bit error probability is always reduced by the independent time slotting. If the transmitters are peak-power limited, a comparison of equations (53) and (59) indicates that

$$N < 1 + \left( \frac{R_s'}{R_s} - 1 \right) \left( \frac{bR_s T_p}{N_0} + 1 \right) \quad (60)$$

is necessary for independent time slotting to be helpful. Since  $N > 1$ , equation (60) cannot be satisfied unless  $R_s' > R_s$ .

A time-hopping system is a system in which the time slots are selected according to the state of a pseudonoise code generator. Figure 11 diagrams a time-hopping pseudonoise system. The data bits are temporarily stored for transmission at a high rate during the slot. After code synchronization has been established at the receiver, only signals corresponding to the desired portion of the frame pass through the initial switch. The pseudonoise nature of the transmitted bursts is useful as a countermeasure to interception or jamming.

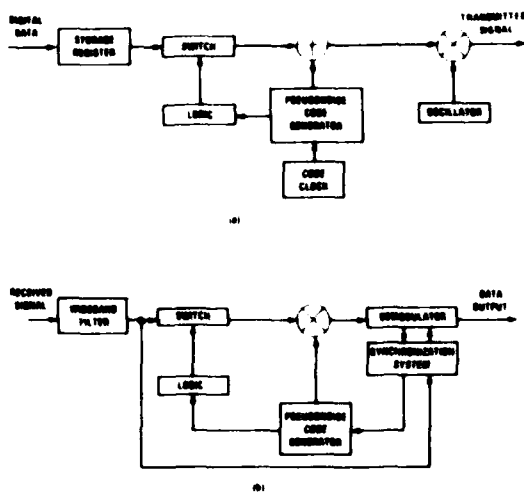


Figure 11. Time-hopping pseudonoise system: (a) transmitter and (b) receiver.

### 3. JAMMING

The jamming resistance of a pseudonoise system depends upon the integrity of its pseudonoise code since, once the code is known, it can be reproduced as a jamming waveform that is not eliminated by the processing gain. To make decipherment time-consuming, the codes should be

long. However, since eventual decipherment is inevitable, the pseudonoise code generators in the transmitter and the receiver must be readily programmable.

Assuming that the pseudonoise code is unknown to the jammer, the most effective form of jamming against a pseudonoise system is tone jamming at the center frequency of the pseudonoise spectrum. For this ideal jamming, the interference parameter is  $b = 1$ . However, if the processing gain is inadequate to eliminate the jamming, there are a number of specific countermeasures against tone jamming. The tone frequency can be acquired by a phase-locked loop sweeping through the pseudonoise bandwidth. The tone can then be subtracted from the received signal to cancel the interference. Alternatively, an adaptive or fixed notch filter can be used as a countermeasure.

If the carrier frequency and the chip rate of a pseudonoise system can be approximately determined by the jammer, then jamming with a pseudonoise signal having a similar carrier frequency and chip rate yields an interference parameter that is  $b = 2/3$ . Although the interference parameter is somewhat lower than for ideal jamming, it is difficult to design a specific countermeasure to supplement the processing gain in suppressing pseudonoise jamming.

### 6. CODE SYNCHRONIZATION

For message demodulation to occur in a pseudonoise receiver, the code must be synchronized to within one chip. Range uncertainty and relative clock drifts are the primary sources of synchronization errors, particularly for mobile communicators. Code synchronization consists of two operations, acquisition and tracking. Acquisition, also called initial synchronization or course synchronization, is the operation by which the relative timing of the receiver code is brought to within one chip of the transmitted code. After this condition is recognized and confirmed, the tracking system is activated. Tracking, also called fine synchronization, is the operation by which syn-

chronization errors are further reduced or at least maintained within one chip.

The acquisition stage is particularly susceptible to hostile actions, whereas the tracking stage is much less sensitive. Thus, we give a brief account of acquisition systems only. Tracking systems have been analyzed by Simon.<sup>9</sup> There are three requirements of an acquisition system for military applications:

- a. Since successful jamming during acquisition completely disables a communication system, the acquisition system must have a strong capability to reject interference.
- b. The pseudonoise codes used for acquisition must be changeable and sufficiently long for security.
- c. The acquisition operation should be rapid so that a jammer must operate continuously to ensure jamming during acquisition; continuous operation reduces the amount of jamming power that can be produced.

The first requirement makes unattractive a number of possible acquisition techniques such as sequential estimation or the use of acquirable codes.<sup>1</sup> Thus, two acquisition techniques appear to be the most desirable for military communications: serial search synchronization and matched-filter synchronization.<sup>1,2</sup>

Serial search synchronization consists of a search over all possible relative time alignments of a received code and a code generated in the receiver. The relative alignments are tested successively until the codes are aligned within a chip. Figure 12 diagrams a serial acquisition system. The received pseudonoise waveform is multiplied by a code generated in the receiver. The latter code has its rate adjusted until the codes are aligned.

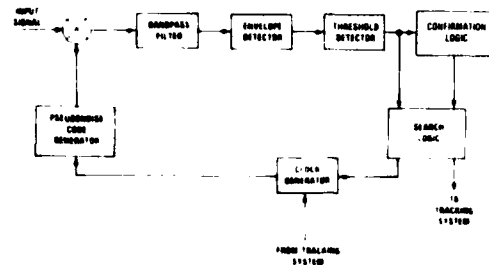


Figure 12. Serial acquisition system.

With the alignment, an envelope detector output exceeds a threshold. Under certain conditions determined by the search logic, the output of the threshold detector stops the search by stabilizing the clock rate. The two codes are temporarily assumed to be in synchronism so the tracking system immediately begins operation. Acquisition is confirmed by logic circuits that continue to monitor the threshold detector output. If confirmation fails, the search operation is resumed.

The spectrum of the local pseudonoise code is shown in figure 8. If tone jamming is present, the input to the bandpass filter of figure 12 contains discrete frequency components. If the code period is such that only one or two of these frequency components pass through the filter, the effect on the envelope detector output can be much greater than that due to random noise with the same power. Thus, to reject interference, the code repetition rate must be much less than the bandwidth of the bandpass filter.

To minimize the noise or interference power that enters the envelope detector, the bandwidth of the bandpass filter should be as small as possible. If Doppler shifts and relative oscillator drifts cause a large uncertainty in the carrier frequency to be received, it may be desirable to replace the bandpass filter, the envelope detector, and the threshold detector by an array of similar devices in parallel. In this manner, the bandwidth of each filter can be kept small.

The pseudonoise code used for acquisition does not have to be the same as the code used for communication following acquisition. Once acquisition occurs, the receiver's code generator for

<sup>1</sup>R. C. Dixon, *Spread Spectrum Systems*, John Wiley and Sons, Inc., New York (1976).

<sup>2</sup>*Spread Spectrum Communications*, NATO Advisory Group for Aerospace Research and Development, National Technical Information Service AD766914 (1976).

<sup>9</sup>M. R. Simon, *Non-coherent Pseudonoise Code Tracking Performance of Spread Spectrum Receivers*, IEEE Trans. Comm., COM-25 (March 1977), 327.

communication can be started at a predetermined point. To reduce the acquisition time, the code sequence length during acquisition can be shorter than the code sequence length during communication. However, if the code period is too short, a serial search acquisition system becomes susceptible to tone jamming. Furthermore, the possibility of either false correlations or code reproduction by a jammer increases as the code sequence length is decreased.

The output of a filter matched to the pseudonoise code can be used to synchronize the receiver code generator. The matched filter can precede or follow a demodulator, depending upon the requirements of the filter design. Figure 13 diagrams a matched-filter acquisition system with protection against interference. The signal matched-filter output is compared with a threshold that is automatically adjusted as a function of a reference matched filter output. The comparator output activates the tracking system and the confirmation logic. Since the reference matched filter produces a relatively small response to the pseudonoise code being used for acquisition, its output is a measure of the interference and the noise. The level adjustment circuit provides amplification or attenuation of the reference matched-filter output according to the desired probabilities of false alarm and detection.

If  $KT_p = T_m$  in a direct-sequence system, a matched-filter output can be used for message demodulation, thereby eliminating the need for a separate code synchronization subsystem.<sup>3</sup> However, the code sequence length required is usually too short to provide the protection against pseudonoise jamming and the security desired in a military communication system.

## 7. HYBRID SYSTEM

A hybrid frequency-hopping pseudonoise system is a pseudonoise system in which the carrier frequency changes periodically. The hybrid system takes advantage of the fact that it is possible to

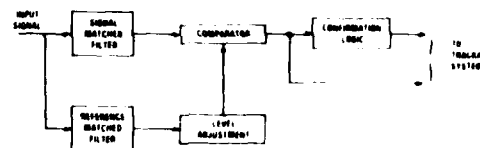


Figure 13. Matched-filter acquisition system with protection against interference.

hop in frequency over a much greater bandwidth than the bandwidth of a pseudonoise waveform. Thus, the hybrid system can spread energy over a much greater bandwidth than a pseudonoise system.

The hybrid system combats narrowband or partial-band interference in two ways. The hopping allows the avoidance of the interference spectrum part of the time. When the system hops into the interference, the interference is spread and filtered as in a pseudonoise system. These features of hybrid systems also help them reduce the effects of mutual interference in a network.

Figure 14 diagrams a hybrid system. In the transmitter, a single pseudonoise code generator controls the spreading and the choice of hopping frequencies. Hops occur periodically after a fixed number of chips. In the receiver, the frequency hopping and the pseudonoise code are removed in succession to produce a carrier with the biphase message modulation.

The presence of the frequency synthesizers allows generation of a frequency-hopping preamble for acquisition. The preamble consists of a code-controlled tone that periodically changes in frequency. The duration of the tone is much greater than that of a chip. Therefore, the timing accuracy requirements at the receiver for preamble synchronization are much less stringent than for the pseudonoise code used for communication. As a result, the initial acquisition, which provides alignment of the hopping frequencies, is relatively rapid. If a hop occurs every  $h$  chips, then initial acquisition aligns the receiver's pseudonoise code within  $h$  chips. A second stage of acquisition over the remaining code timing uncertainty finishes acquisition relatively rapidly since  $h$  is much less than the code sequence length. Thus, the overall

<sup>3</sup>M. G. Unkauf, in *Surface Wave Filters*, H. Matthews, ed., John Wiley and Sons, Inc., New York (1977).

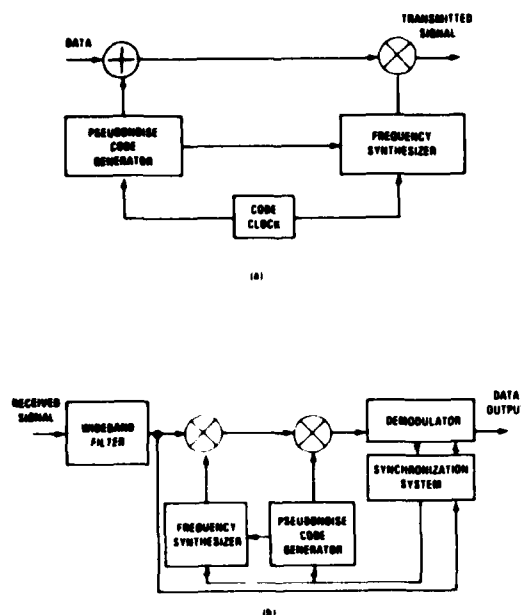


Figure 14. Hybrid frequency-hopping pseudonoise system: (a) transmitter and (b) receiver.

acquisition time for practical hybrid systems is less than the acquisition time for a pseudonoise system with the same code generator.

## 8. COMPARISON WITH FREQUENCY HOPPING

Aside from hybrid systems, the two major candidates for communications that resist jamming and interception are pseudonoise systems and frequency-hopping systems. We compare the word error probabilities of a pseudonoise system with an ideal frequency-hopping system having bit interleaving and differentially coherent minimum-shift keying as the data modulation.<sup>10</sup> We assume that the transmission power, the information rate, and the total available bandwidth are the same for both systems. The channel bandwidth of the frequency-hopping system is  $B_m$ , and we set  $B_m T_m = 1$ . Thus, the processing gain of the pseudonoise system is equal to the number of channels of the frequency-hopping system. We

assume the presence of a single narrowband jamming signal at the center frequency of the available bandwidth so that  $b = 1$ . Figures 15 and 16 show comparisons of  $P_w$  as a function of the signal-to-noise ratio per word for  $G = 1000$  and  $w = 4$ . In figure 15,  $c = 4$  and  $r = 1$ ; in figure 16,  $c = 7$  and  $r = 2$ . As the jamming-to-signal ratio,  $R_j/R_s$ , is increased, the frequency-hopping  $P_w$  is essentially unchanged, whereas the pseudonoise  $P_w$  increases rapidly. A characteristic of frequency-hopping systems is that the errors occur primarily when the system hops into a jammed channel. An increase in the jamming energy beyond a certain level has little effect. In contrast, pseudonoise systems spread narrowband jamming energy over the total bandwidth. An increase in the jamming energy has a direct effect on the probability of an error. A comparison of figures 15 and 16 shows that block coding is much more helpful for the frequency-hopping system than for the pseudonoise system.

Although the figures illustrate important differences in error rate performance between frequency-hopping systems and pseudonoise systems, we cannot draw conclusions for at least two

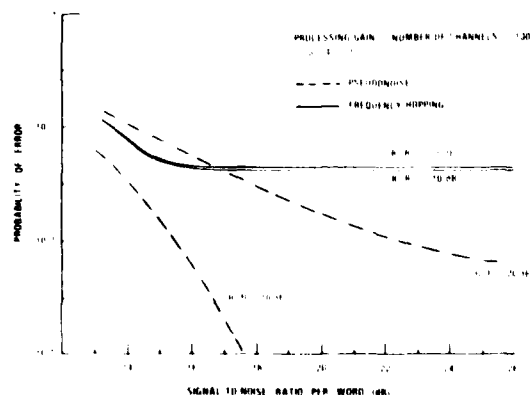


Figure 15. Comparison of uncoded word error probabilities for pseudonoise and frequency hopping in presence of narrowband jamming at center frequency;  $w$  = number of data bits,  $c$  = number of code bits,  $r$  = number of bit errors required for word error,  $R_j$  = total interference power, and  $R_s$  = average power in intended transmission.

<sup>10</sup>D. J. Torrieri, *Simultaneous Mutual Interference and Jamming in a Frequency Hopping Network*, U.S. Army Materiel Development and Readiness Command (CM CCM 80-1, June 1980).

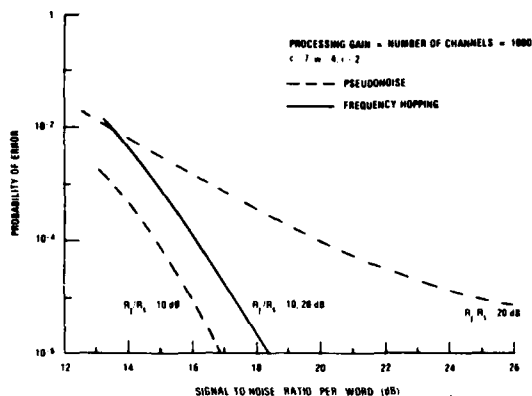


Figure 16. Comparison of coded word error probabilities for pseudonoise and frequency hopping in presence of narrowband jamming at center frequency;  $w$  = number of data bits,  $c$  = number of code bits,  $r$  = number of bit errors required for word error,  $R_j$  = total interference power, and  $R_s$  = average power in intended transmission.

reasons. First, we have considered optimal jamming against the pseudonoise system. For the parameter values chosen, partial-band jamming over a number of channels is far more effective jamming against a frequency-hopping system than narrowband jamming.<sup>10</sup> Second, by equating the total bandwidths of the two systems, we have not allowed for the fact that it is possible to hop in frequency over a much greater bandwidth than the bandwidth of a pseudonoise waveform. Thus, the nature of the jamming threat and constraints upon the potential total bandwidth are crucial considerations in deciding the relative merits of the two systems with respect to error rates.

An advantage of frequency hopping is that acquisition of frequency-hopping synchronization is generally much more rapid and inherently more jam resistant than the acquisition of pseudonoise synchronization.

The relative performances of a pseudonoise network and a frequency-hopping network depend upon the deployment of the network elements and

<sup>10</sup>D. J. Torrieri, *Simultaneous Mutual Interference and Jamming in a Frequency Hopping Network*, U.S. Army Materiel Development and Readiness Command CM/CCM-80-3 (June 1980)

the degree of network coordination. When there are potentially large power differentials at the receivers between desired and interfering signals, frequency-hopping systems are usually degraded less by mutual interference than are comparable pseudonoise systems. When the power differentials are small, pseudonoise systems are usually preferable.

The interceptions of pseudonoise signals and frequency-hopping signals are difficult to compare. A key factor is the hopping rate, which makes detection, frequency estimation, and direction finding more difficult as the rate increases.<sup>6</sup>

## 9. CONCLUSIONS

Pseudonoise spread spectrum systems provide message privacy, multipath protection, transmission concealment, and interference rejection. The effectiveness of pseudonoise systems depends largely upon the characteristics of the pseudonoise code used to spectrally spread the transmitted energy.

Transmission concealment requires that the code period be at least as long as a data bit duration. Security requirements usually limit the shortness of the code sequence and, hence, the code period even more. If the same code is used for both transmission and acquisition, the code period has an upper bound that is determined by the maximum acceptable acquisition time.

The processing gain, which is the ratio of the code bandwidth to the message bandwidth, is a measure of how well a pseudonoise system can reject interference. The most destructive type of interference or jamming exists when the interference power is concentrated at the carrier frequency of the spread spectrum signal. The relative effectiveness of other types of interference is measured by the interference parameter, which is used in error rate calculations.

Error-correcting codes are sometimes helpful in reducing the word error probabilities of pseudo-

<sup>6</sup>D. J. Torrieri, *Interception of Hostile Communications*, U.S. Army Materiel Development and Readiness Command CM/CCM79-3 (October 1979)



noise systems. However, when the total bandwidth and the word duration are fixed, the potential improvement in performance due to encoding is partially counterbalanced by the decrease in processing gain, which results from the increased transmitted bit rate.

The mutual interference between elements in a network of pseudonoise systems can often be reduced by time-division multiplexing. The degree of improvement is dependent upon the coordination among the elements and the peak-power limits during transmission.

Specific countermeasures can be used against tone jamming at the carrier frequency of the spread spectrum signal. Thus, jamming with a pseudonoise waveform is an attractive choice for the jammer if it is possible to measure the carrier frequency and the chip rate of the communications to be jammed.

Among the most desirable code acquisition techniques for military communications are serial search synchronization and matched filter synchronization. The use of a separate, relatively short pseudonoise code during acquisition reduces the acquisition time.

Hybrid frequency-hopping pseudonoise systems take advantage of the superior spreading and acquisition capabilities of frequency hopping while retaining the basic characteristics of pseudonoise systems.

In choosing between pseudonoise and frequency-hopping systems, crucial factors to be considered are the nature of the jamming threat, frequency and bandwidth constraints, the deployment and the coordination of network elements, and the interception threat.

## LITERATURE CITED

1. R. C. Dixon, *Spread Spectrum Systems*, John Wiley and Sons, Inc., New York (1976).
2. *Spread Spectrum Communications*, NATO Advisory Group for Aerospace Research and Development, National Technical Information Service AD766914 (1973).
3. M. G. Unkauf, in *Surface Wave Filters*, H. Matthews, ed., John Wiley and Sons, Inc., New York (1977).
4. W. C. Lindsey and M. K. Simon, *Telecommunication Systems Engineering*, Prentice-Hall, Inc., Englewood Cliffs, NJ (1973).
5. S. Haykin, *Communication Systems*, John Wiley and Sons, Inc., New York (1978).
6. D. J. Torrieri, *Interception of Hostile Communications*, U.S. Army Materiel Development and Readiness Command CM/CCM-79-3 (October 1979).
7. R. E. Ziemer and W. H. Tranter, *Principles of Communications*, Houghton-Mifflin Co., Boston (1976).
8. Special Issue on Spread Spectrum Communications, *IEEE Trans. Comm.*, COM-25 (August 1977).
9. M. K. Simon, Noncoherent Pseudonoise Code Tracking Performance of Spread Spectrum Receivers, *IEEE Trans. Comm.*, COM-25 (March 1977), 327.
10. D. J. Torrieri, Simultaneous Mutual Interference and Jamming in a Frequency Hopping Network, U.S. Army Materiel Development and Readiness Command CM/CCM-80-3 (June 1980).

## GLOSSARY OF PRINCIPAL SYMBOLS

$A$	Amplitude of signal	$R_i(\tau)$	Autocorrelation of $i(t)$
$A_i$	Amplitude of interference	$R_j$	Total interference power
$B_m$	Bandwidth of binary message sequence	$R_j(\tau)$	Autocorrelation of $j(t)$
$B_p$	Bandwidth of received signal	$R_{jp}(\tau)$	Autocorrelation of $j(t)p(t)$
$b$	Interference parameter	$R_m(\tau)$	Autocorrelation of $m(t)$
$c$	Number of code bits in word	$R_n(\tau)$	Autocorrelation of $n(t)$
$E_b$	Energy per bit	$R_p(\tau)$	Autocorrelation of $p(t)$
$F\{ \}$	Fourier transform	$R_s$	Average power in intended transmission
$f_0$	Carrier frequency (hertz) of pseudo-noise signal	$\bar{R}_s(\tau)$	Average autocorrelation of $s(t)$
$f_i$	Carrier frequency (hertz) of interference	$R_s'$	Received signal power from transmitter during one of its time slots
$G$	Processing gain	$R_x(\tau)$	Autocorrelation of periodic function
$i(t)$	Total interference entering matched filter	$r$	Number of bit errors for word error at receiver output
$j(t)$	Received interference	$r(t)$	Total received signal
$K$	Pseudonoise code length	$S_i(f)$	Power spectral density of $i(t)$
$m(t)$	Binary message sequence	$S_j(f)$	Power spectral density of $j(t)$
$N$	Number of elements in network	$S_{jp}(f)$	Power spectral density of $j(t)p(t)$
$N_0$	Twice noise power spectral density	$S_m(f)$	Power spectral density of $m(t)$
$n(t)$	Thermal noise	$S_n(f)$	Power spectral density of $n(t)$
$P_b$	Probability of bit error	$S_p(f)$	Power spectral density of $p(t)$
$P_c$	Probability of error in encoded bit	$\bar{S}_s(f)$	Average power spectral density of $s(t)$
$P_w$	Probability of word error	$s(t)$	Received pseudonoise signal
$p(t)$	Binary pseudonoise code sequence	$T_m$	Duration of message bit
$q(t)$	Interfering pseudonoise sequence		

# GLOSSARY OF PRINCIPAL SYMBOLS (Cont'd)

$T_p$	Duration of chip	$\theta$	Phase angle of pseudonoise signal
$T_q$	Bit duration of $q(t)$	$\Lambda( )$	Triangular pulse, defined by equation (4)
$T_0$	Duration defined by equation (43)	$\omega_0$	Carrier frequency (radians per second) of pseudonoise signal
$T_1$	Duration defined by equation (46)	$\omega_1$	Carrier frequency (radians per second) of interference
$w$	Number of data bits in word		
$\delta( )$	Dirac delta function		

# DISTRIBUTION

ADMINISTRATOR  
DEFENSE DOCUMENTATION CENTER  
ATTN DDC-TCA (12 COPIES)  
CAMERON STATION, BUILDING 5  
ALEXANDRIA, VA 22314

COMMANDER  
US ARMY MISSILE & MUNITIONS  
CENTER AND SCHOOL  
ATTN ATSK-CTD-F  
REDSTONE ARSENAL, AL 35809

DIRECTOR  
US ARMY MATERIEL SYSTEMS ANALYSIS  
ACTIVITY  
ATTN DRXS-MP  
ATTN DRXS-CT  
ABERDEEN PROVING GROUND, MD 21005

DIRECTOR  
DEFENSE ADVANCED RESEARCH PROJECTS  
AGENCY  
ATTN DIR, TACTICAL TECHNOLOGY OFFICE  
ARCHITECT BUILDING  
1400 WILSON BLVD  
ARLINGTON, VA 22209

DIRECTOR  
DEFENSE COMMUNICATIONS ENGINEERING  
CENTER  
ATTN R&D OFFICE, ASST DIR FOR TECH  
1860 WIEHLE AVE  
RESTON, VA 22090

DIRECTOR OF DEFENSE  
RESEARCH & ENGINEERING  
ATTN DEP DIR (TACTICAL WARFARE PROGRAM)  
WASHINGTON, DC 20301

ASSISTANT SECRETARY OF THE ARMY  
(RES, DEV, & ACQ)  
ATTN DEP FOR COMM & TARGET ACQ  
ATTN DEP FOR AIR & MISSILE DEFENSE  
WASHINGTON, DC 20310

COMMANDER  
US ARMY COMMUNICATIONS-ELEC. COMMAND  
ATTN STEEP-MT-M  
FORT HUACHUCA, AZ 85613

OFFICE, DEPUTY CHIEF OF STAFF FOR  
OPERATIONS & PLANS  
DEPARTMENT OF THE ARMY  
ATTN DAMO-TCO, ELECTRONIC/WARFARE  
SIGNAL SECURITY  
ATTN DAMO-RQZ  
WASHINGTON, DC 20310

COMMANDER  
US ARMY CONCEPTS ANALYSIS AGENCY  
8120 WOODMONT AVENUE  
ATTN MDCA-SMS  
BETHESDA, MD 20014

COMMANDER  
US ARMY COMMUNICATIONS R&D COMMAND  
ATTN DRSEL-CE, COMMUNICATIONS-ELECTRONIC  
SYS INTEG OFFICE  
FORT MONMOUTH, NJ 07703

DIRECTOR, ELECTRONIC WARFARE LABORATORY  
ATTN DELEW-V  
ATTN DELEW-C  
ATTN DELEW-E  
ATTN DELEW-M-ST  
FORT MONMOUTH, NJ 07703

COMMANDER  
ELECTRONICS WARFARE LABORATORY  
OFFICE OF MISSILE ELECTRONIC WARFARE  
WHITE SANDS MISSILE RANGE, NM 88002

COMMANDER  
NAVAL WEAPONS CENTER  
ATTN CODE 35, ELECTRONIC WARFARE DEPT  
CHINA LAKE, CA 93555

DIRECTOR  
NAVAL RESEARCH LABORATORY  
ATTN CODE 5700, TACTICAL ELEC  
WARFARE DIVISION  
WASHINGTON, DC 20375

COMMANDER  
NAVAL SURFACE WEAPONS CENTER  
ATTN DF-20, ELECTRONICS WARFARE DIV  
ATTN DK, WARFARE ANALYSIS DEPT  
DAHLGREN, VA 22448

DIRECTOR  
AF AVIONICS LABORATORY  
ATTN KL (WR), ELECTRONIC WARFARE DIV  
WRIGHT-PATTERSON AFB, OH 45433

COMMANDER  
HQ, TACTICAL AIR COMMAND  
ATTN DOR, DIR OF ELECTRONIC  
WARFARE OPNS  
LANGLEY AFB, VA 23665

COMMANDER  
HQ USAF TACTICAL AIR WARFARE  
CENTER (TAC)  
ATTN ER, DCS/ELECTRONIC WARFARE  
AND RECONNAISSANCE  
ATTN ERW, DIR OF ELECTRONIC  
WARFARE  
EGLIN AFB, FL 32542

DISTRIBUTION (Cont'd)

US ARMY ELECTRONICS RESEARCH &  
DEVELOPMENT COMMAND  
ATTN TECHNICAL DIRECTOR, DRDEL-CT  
ATTN DRDEL-CCM (3 COPIES)  
ATTN DRDEL-ST  
ATTN DRDEL-OP  
ATTN TORRIERI, D., DRDEL-CCM (20 COPIES)  
ADELPHI, MD 20783

INSTITUTE FOR DEFENSE ANALYSIS  
400 ARMY NAVY DRIVE  
ARLINGTON, VA 22209

DIA  
DEP DIR OF SCIENTIFIC AND TECH INST  
ELECTRONICS WARFARE BRANCH  
1735 N. LYNN STREET  
ARLINGTON, VA 22209

DEPT OF NAVY  
OFFICE OF RES, DEV, TEST & EVAL  
ATTN TACTICAL AIR SURFACE & EW DEV DIV  
(NOP-982E5)  
ATTN C&C EW AND SENSORS SEC  
(NOP-982F3)  
THE PENTAGON  
WASHINGTON, DC 20350

COMMANDER  
US ARMY TRAINING & DOCTRINE COMMAND  
ATTN ATDC (DCS, COMBAT DEVELOPMENTS)  
FT MONROE, VA 23651

OFFICE OF THE DEPUTY CHIEF OF STAFF  
FOR RES, DEV, & ACQ  
DEPARTMENT OF THE ARMY  
ATTN DAMA-WS  
ATTN DAMA-CS  
ATTN DAMA-AR  
ATTN DAMA-SCS, ELECTRONIC WARFARE TEAM  
WASHINGTON, DC 20310

US ARMY COMBINED ARMS COMBAT DEV ACTIVITY  
ATTN ATZLCA-CA  
ATTN ATZLCA-CO  
ATTN ATZLCA-FS  
ATTN ATZLCA-SW  
ATTN ATZLCA-COM-G  
FT LEAVENWORTH, KS 66027

DIRECTOR  
ELECTRONICS TECHNOLOGY & DEV LAB  
ATTN DELET  
FT MONMOUTH, NJ 07703

COMMANDER  
US ARMY MATERIEL DEV & READINESS COMMAND  
ATTN DRCPP  
ATTN DRCPS  
ATTN DRCDE  
ATTN DECDE-D  
ATTN DRCBSI  
5001 EISENHOWER AVENUE  
ALEXANDRIA, VA 22333

DIRECTOR  
US ARMY NIGHT VISION AND ELECTRO-OPTICS  
LABORATORY  
FT BELVOIR, VA 22060

COMMANDER  
US ARMY COMBAT SURVEILLANCE AND  
TARGET ACQUISITION LAB  
FT MONMOUTH, NJ 07703

DIRECTOR  
US ARMY SIGNALS WARFARE LAB  
VINT HILL FARMS STATION  
WARRENTON, VA 22186

COMMANDER  
US ARMY INTELLIGENCE AND SECURITY COMMAND  
ARLINGTON HALL STATION  
ATTN IARDA (DCS, RDA)  
ATTN IAITA (DIR, THREAT ANALYSIS)  
4000 ARLINGTON BLVD  
ARLINGTON, VA 22212

US ARMY TRADOC SYSTEMS ANALYSIS  
ACTIVITY  
ATTN ATAA-TDB  
WHITE SANDS MISSILE RANGE, NM 88002

DIRECTOR  
NATIONAL SECURITY AGENCY  
ATTN S65  
FT MEADE, MD 20755

HARRY DIAMOND LABORATORIES  
ATTN 00100, CO/TD/TSO/DIVISION DIRECTORS  
ATTN RECORD COPY, 81200  
ATTN HDL LIBRARY, 81100 (3 COPIES)  
ATTN HDL LIBRARY, 81100 (WRF)  
ATTN TECHNICAL REPORTS BR, 81300  
ATTN FEMENIAS, R., 22100  
ATTN SANN, K., 11100  
ATTN FAZI, C., 11400  
ATTN GORNAK, G., 21200  
ATTN INGERSOLL, P., 34300  
ATTN WALSH, G., 15300

TE  
ED  
80